AMENDMENTS TO THE CLAIMS

1. (Currently amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one dynamic behavior evaluation module, wherein each dynamic behavior evaluation module provides a virtual environment for executing a code module of a particular type, and wherein each dynamic behavior evaluation module records some execution behaviors of the code module as it is executed, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module;

a management module for obtaining the code module and selecting a dynamic behavior evaluation module to execute the code module according to the code module's type;

a malware behavior signature store storing at least one known malware behavior signature of a known malware; and

a behavior signature comparison module that obtains the behavior signature of the code module and compares the behavior signature of the code module to the known malware behavior signatures in the malware behavior signature store to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware.

2. (Currently amended) A malware detection system for determining whether a code module is malware according to the code module's exhibited behaviors, the system comprising:

at least one behavior evaluation means, wherein each behavior evaluation means provides a virtual environment for executing a code module of a particular type, and wherein each behavior evaluation means records some execution behaviors of the code module as it is executed, wherein the execution behaviors of the code module are recorded into a behavior signature corresponding to the code module;

a management means for obtaining the code module and selecting a behavior evaluation means to execute the code module according to the code module's type;

a storage means for storing at least one known malware behavior signature of a known malware; and

a behavior comparison means for comparing the behavior signature of the code module to the known malware behavior signatures in the storage means to determine whether the exhibited execution behaviors of the code module match the exhibited execution behaviors of a known malware.

3. (Previously presented) A method for determining whether a code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module during execution of the code module;

comparing the recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware execution behaviors; and

according to the results of the previous comparison, determining whether the code module is malware.

4. (Previously presented) A computer-readable medium bearing computer-executable instructions which, when executed, carry out a method for determining whether an executable code module is malware according to the code module's exhibited behaviors, the method comprising:

selecting a dynamic behavior evaluation module according to the executable type of the code module;

executing the code module in the selected dynamic behavior evaluation module, wherein the selected dynamic behavior evaluation module provides a virtual environment in which the code module may be safely executed;

recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module as the code module is executing;

comparing the recorded execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module to known malware execution behaviors; and

according to the results of the previous comparison, determining whether the code module is malware.

5. (Previously presented) The malware detection system of Claim 1, wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

6. (Previously presented) The malware detection system of Claim 5, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

7. (Previously presented) The malware detection system of Claim 6, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

8. (Previously presented) The malware detection system of Claim 2, wherein recording some execution behaviors of the code module as it is executed comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

9. (Previously presented) The malware detection system of Claim 8, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

10. (Previously presented) The malware detection system of Claim 9, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

11. (Previously presented) The method of Claim 3, wherein recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

12. (Previously presented) The method of Claim 11, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

13. (Previously presented) The method of Claim 12, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.

14. (Previously presented) The computer-readable medium of Claim 4, wherein recording some execution behaviors exhibited by the code module executing in the dynamic behavior evaluation module comprises recording executed behaviors that are identified in a predefined set of execution behaviors to record.

15. (Previously presented) The computer-readable medium of Claim 14, wherein the predefined set of execution behaviors to record corresponds to the dynamic behavior evaluation module in which a code module of a particular type may be executed.

16. (Previously presented) The computer-readable medium of Claim 14, wherein the predefined set of execution behaviors to record corresponds to a set of system calls.